Biometric Authentication Overview

1. Aim

From the casual users of the home computer to the business, corporations and government, there is a great concern about the security of files, systems, and the ability of technology to protect us from unauthorized access. Computer software companies have put a great effort to meet the demand for better security of sensitive, confidential, and classified information. This is where the biometric technology is getting widely adopted. In recent years there has been considerable growth in interest in the use of biometric systems for personal authentication. By using biometrics, authentication is directly linked to the person, rather than their token or password.

Biometric authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. Biometric samples include fingerprints, retinal scans, face recognition, voice prints and even typing patterns. In this article, we will discuss the concept of biometric authentication, the different types of biometric authentication, compare their pros and cons and the technology current maturity level. Finally, we will conclude our paper with findings and recommendations on how biometric authentication could be used in the university.

2. Biometric Authentication Overview

2.1 What is Biometrics

Biometrics refers to metrics related to human characteristics, it is a field of technology which has been used in the identification of individuals based on some physical attribute. Biometrics covers a variety of technologies in which unique identifiable attributes of people are used for identification and authentication. These include (but are not limited to) a person's fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals seeking to control access to computers, airlines, databases and other areas which may need to be restricted.

2.2 Types of Biometric Authentication

There are many different types of biometrics, which can be used in authentication and security, typically include the following:

- ***DNA matching:*** the identification of an individual using the analysis of the segments from the person's DNA.
- ***Eyes- iris recognition:*** the use of the features found in the iris to identify an individual.
- ***Eyes - retina recognition:*** the use of patterns of veins in the back of the eye to accomplish recognition.
- ***Face recognition:*** Facial recognition uses algorithms to analyse features. These include the position/size/shape of the eyes, nose, cheekbones and jaw line. Initially, this process was known as 2D facial recognition. The update version is 3D biometric facial recognition. Images are captured with a real-time 3D camera or by digitally scanning a 2D photo. Detailed information like the contour of the eye sockets, nose and cheekbones help make identification easier.
- ***Fingerprint recognition:*** This type of biometrics compares two fingerprints to determine identification. It analyses the ridges and valleys patterns on the fingertip for differences. These fingerprint patterns include the arch, loop, and whorl.
- ***Signature recognition:*** the authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication: static and dynamic. Static is most often a visual comparison between one scanned signature against an ink signature. Dynamic signature is a biometric modality that uses, for recognition purposes, the anatomical and behavioural characteristics that an individual exhibits when signing his or her name (or other phrase).
- ***Typing recognition:*** Keystroke recognition measures the characteristics of an individual's typing pattern, including the time spacing of words. It is the use of the unique characteristics of a person's typing for establishing identity.
- ***Voice recognition:*** Voice recognition is used to discover an unknown speaker's identity based on patterns of voice pitch and speech style. Voice recognition is not the same as speech recognition. Speech recognition

Li Zhao, IT Innovation Specialist
itinnovation@contacts.bham.ac.uk

strips out the personal differences to detect the words, while voice recognition typically disregards the language and meaning to detect the physical person behind the speech.

3. Pros and Cons of Biometric Authentication

Biometric technology has been seen as a breakthrough, however, there are both positives and negatives that can be seen. It is important to evaluate the biometric technology and use them at the right scenarios. In general, biometric technology has the following pros and cons:

Pros of Biometric Technology:

- ***Convenience:*** biometric information is unique and intrinsic to the individual. Users don't need to remember any password or bring any device.
- ***Invaluable resource:*** the database that is being built up with the use of biometric information allows for an invaluable database. For instance, this database can be used to fight crime and terror.
- ***Less Identity fraud:*** biometric information is less likely to be a fraud because of its complexity in nature.

Cons of Biometric Technology:

- ***High Cost:*** biometric devices are much more costly compared to ID cards. Biometric technology is much more effective for security and identification purposes, but it is also much more expensive.
- ***Errors can occur:*** Although biometric technology is very effective and reliable, there are still errors. Currently, the error rate for most biometric device is around 1%.
- ***Injuries and criminal can get around biometric devices:*** since biometrics rely entirely on identifying a unique part of the human body, if there is any injury to that particular part of our body, these biometric devices will not work. This means that biometric devices are not completely effective in halting criminals. Under certain lighting and temperatures, biometric devices are even further impaired.

To further compare the different types of biometric technology, the following table listed the advantages and disadvantages of the biometric technologies.

Biometric Technology	***Advantages***	***Disadvantages***
DNA matching	❖ Very high accuracy ❖ It is standardized	❖ Extremely intrusive ❖ Very expensive
Eyes- iris recognition	❖ Very high accuracy ❖ Verification time is generally less than 5 seconds ❖ The eye of a dead person would deteriorate too fast to be useful, so no extra precautions have to be taken with retinal scans to be sure the user is a living human being	❖ Intrusive ❖ A lot of memory for the data to be stored ❖ Very expensive
Eyes - retina recognition	❖ Very high accuracy ❖ There is no known way to replicate a retina ❖ The eye of a dead person would deteriorate too fast to be useful, so no extra precautions have to be taken with retinal scans to be sure the user is a living human being	❖ Very intrusive ❖ User's acceptance is low, they think it is potentially harmful to the eye ❖ Comparisons of template records can take upwards of 10 seconds, depending on the size of the database ❖ Very expensive
Face Recognition	❖ Non intrusive, contactless ❖ 3D and infrared cameras equal high accuracy ❖ Quick response speed	❖ 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wears glasses ❖ Significant weight changes or changes in appearance will affect the accuracy ❖ Requires camera equipment for user identification
Finger Print	❖ Very high accuracy. ❖ It is the most economical and most	❖ Injury, whether temporary or permanent, can interfere with the scanning process

	developed biometrics ❖ Easy to use. ❖ Small storage space required for the biometric template, reducing the size of the database memory required ❖ It is standardized	❖ It can make mistakes due to the dryness or dirty to the finger's skin, as well as the age ❖ It is intrusive as it is still related to criminal identification
Signature recognition	❖ Non intrusive ❖ Little time of verification (about five seconds) ❖ Low cost	❖ Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification. ❖ Error rate: 1 in 50.
Typing recognition	❖ Non intrusive ❖ No additional cost on hardware	❖ It can make mistakes which may either block access to legitimate users or inadvertently grant access to unauthorized users
Voice recognition	❖ Non intrusive. High social acceptability ❖ Verification time is about five seconds ❖ Low cost	A person's voice can be easily recorded and used for unauthorised PC or network Low accuracy An illness such as a cold can change a person's voice, making absolute identification difficult or impossible

4. Future Work

There are many types of biometric authentication. Different types of biometric authentication will have different best user scenarios. Therefore, to apply the most suitable biometric authentication technology is the key to a successful adoption of biometric authentication. In most cases, biometric authentication technology provides greater convenience, because the user doesn't need to bring any device or remember anything. Another thing to be aware is that biometric authentication technology is at different levels of maturity. For instance, the fingerprint authentication is widely used in the security, whereas face recognition is still on its way to maturity. Overall, it is worthwhile to keep a close eye in the development of biometric authentication and explore the most suitable user scenarios in the university to apply biometric authentication. To further explore biometric authentication technology, IT Innovation Centre already carried out an experiment of using voice authentication for user authentication.

Li Zhao, IT Innovation Specialist
itinnovation@contacts.bham.ac.uk